

Chapter 3: Principles of System Safety

3.1 DEFINITION OF SYSTEM SAFETY	ERROR! BOOKMARK NOT DEFINED.
3.2 PLANNING PRINCIPLES	2
3.3 HAZARD ANALYSIS	3
3.4 COMPARATIVE SAFETY ASSESSMENT	9
3.5 RISK MANAGEMENT DECISION MAKING	12
3.6 SAFETY ORDER OF PRECEDENCE.....	12
3.7 BEHAVIORAL-BASED SAFETY	15
3.8 MODELS USED BY SYSTEM SAFETY FOR ANALYSIS	15

3.0 Principles of System Safety

3.1 Definition of System Safety

System safety is a specialty within system engineering that supports program risk management. It is the application of engineering and management principles, criteria and techniques to optimize safety. The goal of System Safety is to optimize safety by the identification of safety related risks, eliminating or controlling them by design and/or procedures, based on acceptable system safety precedence. As discussed in Chapter 2, the FAA AMS identifies System Safety Management as a Critical Functional Discipline to be applied during all phases of the life cycle of an acquisition. FAA Order 8040.4 establishes a five step approach to safety risk management as: Planning, Hazard Identification, Analysis, Assessment, and Decision. The system safety principles involved in each of these steps are discussed in the following paragraphs.

3.2 Planning Principles

System safety must be planned. It is an integrated and comprehensive engineering effort that requires a trained staff experienced in the application of safety engineering principles. The effort is interrelated, sequential and continuing throughout all program phases. The plan must influence facilities, equipment, procedures and personnel. Planning should include transportation, logistics support, storage, packing, and handling, and should address Commercial Off-the-Shelf (COTS) and Non-developmental Items (NDI). For the FAA AMS applications of system safety, a System Safety Management Plan is needed in the Pre-investment Decision phases to address the management objectives, responsibilities, program requirements, and schedule (who?, what?, when?, where?, and why?). After the Investment Decision is made and a program is approved for implementation, a System Safety Program Plan is needed. See Chapter 5, for details on the preparation of a SSPP.

3.2.1 Managing Authority (MA) Role

Throughout this document, the term Managing Authority (MA) is used to identify the responsible entity for managing the system safety effort. In all cases, the MA is a FAA organization that has responsibility for the program, project or activity. Managerial and technical procedures to be used must be approved by the MA. The MA resolves conflicts between safety requirements and other design requirements, and resolves conflicts between associate contractors when applicable. See Chapter 5 for a discussion on Integrated System Safety Program Plans.

3.2.2 Defining System Safety Requirements

System safety requirements must be consistent with other program requirements. A balanced program attempts to optimize safety, performance and cost. System safety program balance is the product of the interplay between system safety and the other three familiar program elements of cost, schedule, and performance as shown in Figure 3-1. Programs cannot afford accidents that will prevent the achievement of the primary mission goals. However, neither can we afford systems that cannot perform due to unreasonable and unnecessary safety requirements. Safety must be placed in its proper perspective. A correct safety balance cannot be achieved unless acceptable and unacceptable conditions are established early enough in the program to allow for the selection of the optimum design solution and/or operational alternatives. Defining acceptable and unacceptable risk is as important for cost-effective accident prevention as is defining cost and performance parameters.

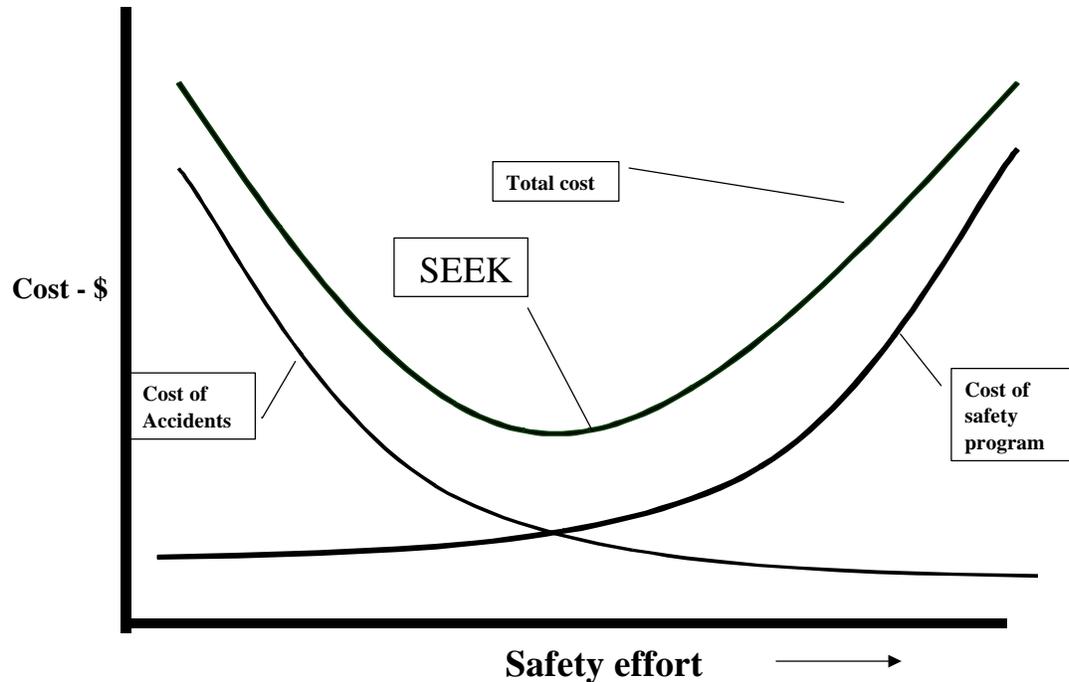


Figure 3-1: Cost vs. Safety Effort (Seeking Balance)

3.3 Hazard Analysis

Both elements of risk (hazard severity and likelihood of occurrence) must be characterized. The inability to quantify and/or lack of historical data on a particular hazard does not exclude the hazard from this requirement¹. The term "hazard" is used generically in the early chapters of this handbook. Beginning with Chapter 7, hazards are subdivided into sub-categories related to environment such as system states, environmental conditions or "initiating" and "contributing" hazards.

Realistically, a certain degree of safety risk must be accepted. Determining the acceptable level of risk is generally the responsibility of management. Any management decisions, including those related to safety, must consider other essential program elements. The marginal costs of implementing hazard control requirements in a system must be weighed against the expected costs of not implementing such controls. The cost of not implementing hazard controls is often difficult to quantify before the fact. In order to quantify expected accident costs before the fact, two factors must be considered. These are related to risk and are the potential consequences of an accident and the probability of its occurrence. The more severe the consequences of an accident (in terms of dollars, injury, or national prestige, etc.) the lower the probability of its occurrence must be for the risk to be acceptable. In this case, it will be worthwhile to spend money to reduce the probability by implementing hazard controls. Conversely, accidents whose consequences are less severe may be acceptable risks at higher probabilities of occurrence and will consequently justify a lesser expenditure to further reduce the frequency of occurrence. Using this concept as a baseline, design limits must be defined.

¹ FAA Order 8040.4 Paragraph 5.c.

3.3.1 Accident Scenario Relationships

In conducting hazard analysis, an accident scenario as shown in Figure 3-2 is a useful model for analyzing risk of harm due to hazards. Throughout this System Safety Handbook, the term hazard will be used to describe scenarios that may cause harm. It is defined in FAA Order 8040.4 as a "Condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event." Seldom does a single hazard cause an accident. More often, an accident occurs as the result of a sequence of causes termed initiating and contributory hazards. As shown in Figure 3-2, contributory hazards involve consideration of the system state (e.g., operating environment) as well as failures or malfunctions. In chapter 7 there is an in-depth discussion of this methodology.

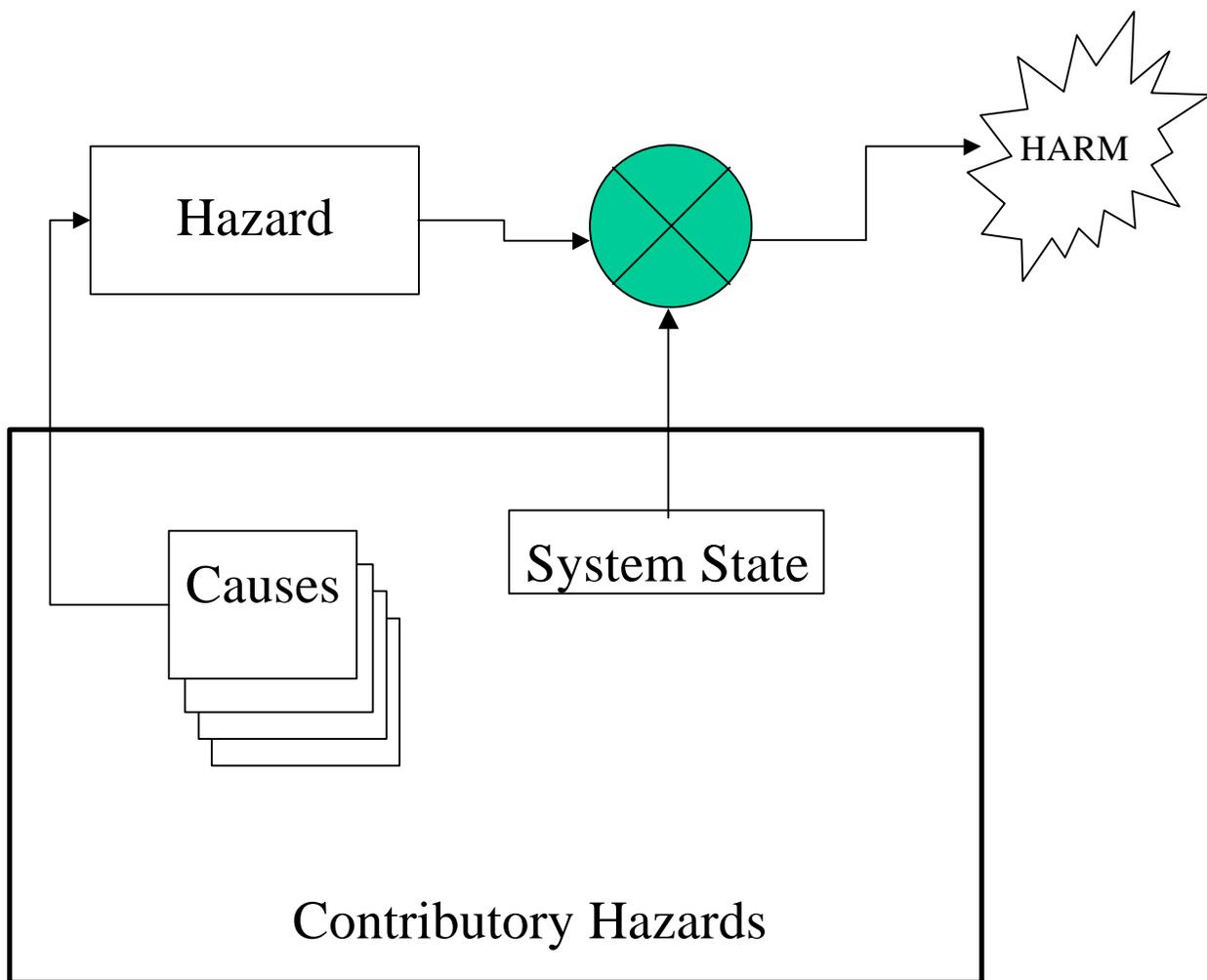


Figure 3-2: Hazard Scenario Model

3.3.2 Definitions for Use in the FAA Acquisition Process

The FAA System Engineering Council (SEC) has approved specific definitions for Severity and Likelihood to be used during all phases of the acquisition life cycle. These are shown in Table 3-2 and Table 3-3.

Table 3-2: Severity Definitions for FAA AMS Process

Catastrophic	Results in multiple fatalities and/or loss of the system
Hazardous	Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be: Large reduction in safety margin or functional capability Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely (1) Serious or fatal injury to small number of occupants of aircraft (except operators) Fatal injury to ground personnel and/or general public
Major	Reduces the capability of the system or the operators to cope with adverse operating condition to the extent that there would be – Significant reduction in safety margin or functional capability Significant increase in operator workload Conditions impairing operator efficiency or creating significant discomfort Physical distress to occupants of aircraft (except operator) including injuries Major occupational illness and/or major environmental damage, and/or major property damage
Minor	Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Include Slight reduction in safety margin or functional capabilities Slight increase in workload such as routine flight plan changes Some physical discomfort to occupants or aircraft (except operators) Minor occupational illness and/or minor environmental damage, and/or minor property damage
No Safety Effect	Has no effect on safety

Table 3-3: Likelihood of Occurrence Definitions

Probable	Qualitative: Anticipated to occur one or more times during the entire system/operational life of an item. Quantitative: Probability of occurrence per operational hour is greater than 1×10^{-5}
Remote	Qualitative: Unlikely to occur to each item during its total life. May occur several time in the life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-5} , but greater than 1×10^{-7}
Extremely Remote	Qualitative: Not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-7} but greater than 1×10^{-9}
Extremely Improbable	Qualitative: So unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-9}

MIL-STD-882 Definitions of Severity and Likelihood

An example taken from MIL-STD-882C of the definitions used to define Severity of Consequence and Event Likelihood are in Tables 3-4 and 3-5, respectively.

Table 3-4: Severity of Consequence

<i>Description</i>	<i>Category</i>	<i>Definition</i>
Catastrophic	I	Death, and/or system loss, and/or severe environmental damage.
Critical	II	Severe injury, severe occupational illness, major system and/or environmental damage.
Marginal	III	Minor injury, minor occupational illness, and/or minor system damage, and/or environmental damage.
Negligible	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Table 3-5: Event Likelihood (Probability)

Description	Level	Specific Event
Frequent	A	Likely to occur frequently
Probable	B	Will occur several times in the life of system.
Occasional	C	Likely to occur some time in the life of the system.
Remote	D	Unlikely but possible to occur in the life of the system.
Inprobable	E	So unlikely, it can be assumed that occurrence may not be experienced.

3.3.3 Comparison of FAR and JAR Severity Classifications

Other studies have been conducted to define severity and event likelihood for use by the FAA. A comparison of the severity classifications for the FARs and JARs from one such study² is contained in Table 3-6. JARs are the Joint Aviation Regulations with European countries.

² Aircraft Performance Comparative Safety Assessment Model (APRAM), Rannoch Corporation, February 28, 2000

Table 3-6 Most Severe Consequence Used for Classification

Probability (Quantitative)	1.0		10^{-3}		10^{-5}		10^{-7}		10^{-9}	
Probability (Descriptive)	FAR		Probable		Improbable				Extremely Improbable	
	JAR	Frequent	Reasonably Probable	Remote	Extremely Remote		Extremely Improbable			
Failure condition severity classification	FAR		Minor		Major				Catastrophic	
	JAR		Minor		Major		Hazardous		Catastrophic	
Effect on aircraft occupants	FAR		<ul style="list-style-type: none"> Does not significantly reduce airplane safety (Slight decrease in safety margins) Crew actions well within capabilities (Slight increase in crew workload) Some inconvenience to occupants 		<ul style="list-style-type: none"> Reduce capability of airplane or crew to cope with adverse operating conditions Significant reduction in safety margins Significant increase in crew workload <p>Severe Cases:</p> <ul style="list-style-type: none"> Large reduction in safety margins Higher workload or physical distress on crew - can't be relied upon to perform tasks accurately Adverse effects on occupants 				<ul style="list-style-type: none"> Conditions which prevent continued safe flight and landing 	
	JAR		Nuisance	<ul style="list-style-type: none"> Operating limitations Emergency procedures 	<ul style="list-style-type: none"> Significant reduction in safety margins Difficulty for crew to cope with adverse conditions Passenger injuries 	<ul style="list-style-type: none"> Large reduction in safety margins Crew extended because of workload or environmental conditions Serious or fatal injury to small number of occupants 	<ul style="list-style-type: none"> Multiple deaths, usually with loss of aircraft 			

3.4 Comparative Safety Assessment

Selection of some alternate design elements, e.g., operational parameters and/or architecture components or configuration in lieu of others implies recognition on the part of management that one set of alternatives will result in either more or less risk of an accident. The risk management concept emphasizes the identification of the change in risk with a change in alternative solutions. Safety Comparative Safety Assessment is made more complicated considering that a lesser safety risk may not be the optimum choice from a mission assurance standpoint. Recognition of this is the keystone of safety risk management. These factors make system safety a decision making tool. It must be recognized, however, that selection of the greater safety risk alternative carries with it the responsibility of assuring inclusion of adequate warnings, personnel protective systems, and procedural controls. Safety Comparative Safety Assessment is also a planning tool. It requires planning for the development of safety operating procedures and test programs to resolve uncertainty when safety risk cannot be completely controlled by design. It provides a control system to track and measure progress towards the resolution of uncertainty and to measure the reduction of safety risk.

Assessment of risk is made by combining the severity of consequence with the likelihood of occurrence in a matrix. Risk acceptance criteria to be used in the FAA AMS process are shown in Figure 3-3 and Figure 3-4.

<i>Severity Likelihood</i>	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Probable A					
Remote B					
Extremely Remote C					
Extremely Improbable D					

High Risk
Medium Risk
Low Risk

Figure 3-3: Risk Acceptability Matrix

	High Risk --Unacceptable. Tracking in the FAA Hazard Tracking System is required until the risk is reduced and accepted.
	Medium -- Acceptable with review by the appropriate management authority. Tracking in the FAA Hazard Tracking System is required until the risk is accepted.
	Low -- Low risk is acceptable without review. No further tracking of the hazard is required.

Figure 3-4: Risk Acceptance Criteria

An example based on MIL-STD-882C is shown in Figure 3-5. The matrix may be referred to as a Hazard Risk Index (HRI), a Risk Rating Factor (RRF), or other terminology, but in all cases, it is the criteria used by management to determine acceptability of risk.

The Comparative Safety Assessment Matrix of Figure 3-5 illustrates an acceptance criteria methodology. Region R1 on the matrix is an area of high risk and may be considered unacceptable by the managing authority. Region R2 may be acceptable with management review of controls and/or mitigations, and R3 may be acceptable with management review. R4 is a low risk region that is usually acceptable without review.

FREQUENCY OF OCCURENCE	HAZARD CATEGORIES			
	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) Frequent	IA	IIA	IIIA	IVA
(B) Probable	R1 IB	IIB	IIIB	IVB
(C) Occasional	IC	IIC	IIIC	IVC R4
(D) Remote	R2 ID	IID	IIID	IVD
(E) Improbable	R3 IE	IIE	IIIEP	IVE
Hazard Risk Index (HRI)				
R1	Suggested Criteria			
R2	Unacceptable			
R3	Must control or mitigate (MA review)			
R4	Acceptable with MA review			
	Acceptable without review			

Figure 3-5: Example of a Comparative Safety Assessment Matrix

Early in a development phase, performance objectives may tend to overshadow efforts to reduce safety risk. This is because sometimes safety represents a constraint on a design. For this reason, safety risk reduction is often ignored or overlooked. In other cases, safety risk may be appraised, but not fully enough to serve as a significant input to the decision making process. As a result, the sudden identification of a significant safety risk, or the occurrence of an actual incident, late in the program can provide an overpowering impact on schedule, cost, and sometimes performance. To avoid this situation, methods to reduce safety risk must be applied commensurate with the task being performed in each program phase.

In the early development phase (investment analysis and the early part of solution implementation), the system safety activities are usually directed toward: 1) establishing risk acceptability parameters; 2) practical tradeoffs between engineering design and defined safety risk parameters; 3) avoidance of alternative approaches with high safety risk potential; 4) defining system test requirements to demonstrate safety characteristics; and, 5) safety planning for follow-on phases. The culmination of this effort is the safety Comparative Safety Assessment that is a summary of the work done toward minimization of unresolved safety concerns and a calculated appraisal of the risk. Properly done, it allows intelligent management decisions concerning acceptability of the risk.

The general principles of safety risk management are:

All system operations represent some degree of risk.

Recognize that human interaction with elements of the system entails some element of risk.

Keep hazards in proper perspective.

Do not overreact to each identified risk, but make a conscious decision on how to deal with it.

Weigh the risks and make judgments according to your own knowledge, inputs from subject matter experts, experience, and program need.

It is more important to establish clear objectives and parameters for Comparative Safety Assessment related to a specific program than to use generic approaches and procedures.

There may be no "single solution" to a safety problem. There are usually a variety of directions to pursue. Each of these directions may produce varying degrees of risk reduction. A combination of approaches may provide the best solution.

Point out to designers the safety goals and how they can be achieved rather than tell him his approach will not work.

There are no "safety problems" in system planning or design. There are only engineering or management problems that, if left unresolved, may lead to accidents.

The determination of severity is made on a "worst credible case/condition" in accordance with MIL-STD-882, and AMJ 25.1309.

- Many hazards may be associated with a single risk. In predictive analysis, risks are hypothesized accidents, and are therefore potential in nature. Severity assessment is made regarding the potential of the hazards to do harm.

3.5 Risk Management Decision Making

For any system safety effort to succeed there must be a commitment on the part of management. There must be mutual confidence between program managers and system safety management. Program managers need to have confidence that safety decisions are made with professional competence. System safety management and engineering must know that their actions will receive full program management attention and support. Safety personnel need to have a clear understanding of the system safety task along with the authority and resources to accomplish the task. Decision-makers need to be fully aware of the risk they are taking when they make their decisions. They have to manage program safety risk. For effective safety risk management, program managers should:

Ensure that competent, responsible, and qualified engineers be assigned in program offices and contractor organizations to manage the system safety program.

Ensure that system safety managers are placed within the organizational structure so that they have the authority and organizational flexibility to perform effectively.

Ensure that all known hazards and their associated risks are defined, documented, and tracked as a program policy so that the decision-makers are made aware of the risks being assumed when the system becomes operational.

Require that an assessment of safety risk be presented as a part of program reviews and at decision milestones. Make decisions on risk acceptability for the program and accept responsibility for that decision.

3.6 Safety Order of Precedence

One of the fundamental principles of system safety is the Safety Order of Precedence in eliminating, controlling or mitigating a hazard. The Safety Order of Precedence is shown in Table 3-7. It will be referred to several times throughout the remaining chapters of this handbook.

Table 3-7: Safety Order of Precedence

Description	Priority	Definition
Design for minimum risk.	1	Design to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through design selection.
Incorporate safety devices.	2	If identified risks cannot be eliminated through design selection, reduce the risk via the use of fixed, automatic, or other safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.
Provide warning devices.	3	When neither design nor safety devices can effectively eliminate identified risks or adequately reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal. Warning signals and their application shall be designed to minimize the likelihood of inappropriate human reaction and response. Warning signs and placards shall be provided to alert operational and support personnel of such risks as exposure to high voltage and heavy objects.
Develop procedures and training.	4	Where it is impractical to eliminate risks through design selection or specific safety and warning devices, procedures and training are used. However, concurrence of authority is usually required when procedures and training are applied to reduce risks of catastrophic, hazardous, major, or critical severity.

Examples:

- Design for Minimum Risk:
Design hardware systems in accordance with FAA-G-2100g, i.e., use low voltage rather than high voltage where access is provided for maintenance activities.
- Incorporate Safety Devices
If low voltage is unsuitable, provide interlocks.
- Provide warning devices
If safety devices are not practical, provide warning placards
- Develop procedures and training
Train maintainers to shut off power before

opening high voltage panels

3.7 Behavioral-Based Safety

Safety management must be based on the behavior of people and the organizational culture. Everyone has a responsibility for safety and should participate in safety management efforts. Modern organization safety strategy has progressed from “safety by compliance” to more of an appropriate concept of “prevention by planning”. Reliance on compliance could translate to after-the-fact hazard detection, which does not identify organizational errors, that are often times, the contributors to accidents.

Modern safety management, i.e.--“system safety management”-- adopts techniques of system theory, statistical analysis, behavioral sciences and the continuous improvement concept. Two elements critical to this modern approach are a good organizational safety culture and people involvement.

The establishment of system safety working groups, analysis teams, and product teams accomplishes a positive cultural involvement when there are consensus efforts to conduct hazard analysis and manage system safety programs.

Real-time safety analysis is conducted when operational personnel are involved in the identification of hazards and risks, which is the key to behavioral-based safety. The concept consists of a “train-the-trainer” format. See chapter 14 for a detailed discussion of how a selected safety team is provided the necessary tools and is taught how to:

- Identify hazards, unsafe acts or conditions;
- Identify “at risk” behaviors;
- Collect the information in a readily available format for providing immediate feedback;
- Train front-line people to implement and take responsibility for day-to-day operation of the program.

The behavioral-based safety process allows an organization to create and maintain a positive safety culture that continually reinforces safe behaviors over unsafe behaviors. This will ultimately result in a reduction of risk. For further information concerning behavioral-based safety contact the FAA’s Office of System Safety.

3.8 Models Used by System Safety for Analysis

The AMS system safety program uses models to describe a system under study. These models are known as the 5M model and the SHELL model. While there are many other models available, these two recognize the interrelationships and integration of the hardware, software, human, environment and procedures inherent in FAA systems. FAA policy and the system safety approach is to identify and control the risks associated with each element of a system on a individual, interface and system level.

The first step in performing safety risk management is describing the system under consideration. This description should include at a minimum, the functions, general physical characteristics, and operations of the system. Normally, detailed physical descriptions are not required unless the safety analysis is focused on this area.

Keep in mind that the reason for performing safety analyses is to identify hazards and risks and to communicate that information to the audience. At a minimum, the safety assessment should describe the system in sufficient detail that the projected audience can understand the safety risks.

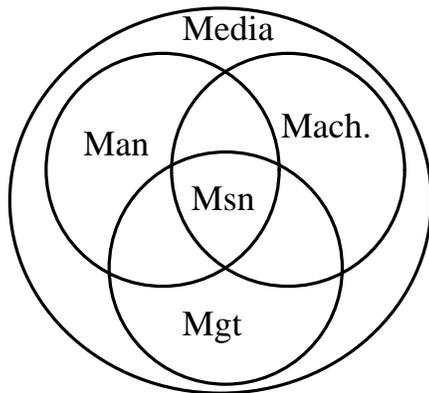
A system description has both breadth and depth. The breadth of a system description refers to the system boundaries. Bounding means limiting the system to those elements of the system model that affect or interact with each other to accomplish the central mission(s) or function. Depth refers to the level of detail in the description. In general, the level of detail in the description varies inversely with the breadth of the system. For a system as broad as the National Airspace System (NAS) our description would be very general in nature with little detail on individual components. On the other hand, a simple system, such as a valve in a landing gear design, could include a lot of detail to support the assessment.

First, a definition of “system” is needed. This handbook and MIL-STD-882¹ (System Safety Program Requirements) define a system as:

A composite at any level of complexity, of personnel, procedures, material, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operation or support environment to perform a given task or achieve a specific production, support, or mission requirement.

Graphically, this is represented by the 5M and SHELL models, which depict, in general, the types of elements that should be considered within most systems.

5M model of System Engineering



- Msn - Mission: central purpose or functions
- Man - Human element
- Mach - Machine: hardware and software
- Media - Environment: ambient and operational environment
- Mgt- Management: procedures, policies, and regulations

Figure 3-6: The Five-M Model

Mission. The mission is the purpose or central function of the system. This is the reason that all the other elements are brought together.

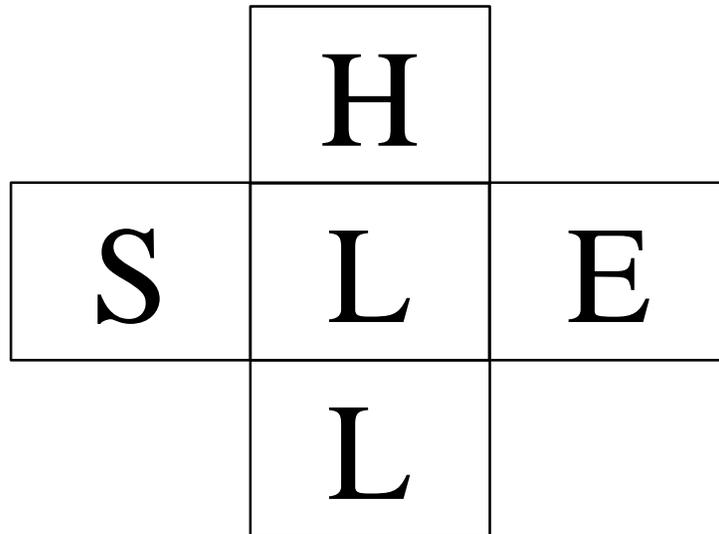
Man. This is the human element of a system. If a system requires humans for operation, maintenance, or installation this element must be considered in the system description.

Machine. This is the hardware and software (including firmware) element of a system.

Management. Management includes the procedures, policy, and regulations involved in operating, maintaining, installing, and decommissioning a system.

(1) **Media.** Media is the environment in which a system will be operated, maintained, and installed. This environment includes operational and ambient conditions. Operational environment means the conditions in which the mission or function is planned and executed. Operational conditions are those involving things such as air traffic density, communication congestion, workload, etc. Part of the operational environment could be described by the type of operation (air traffic control, air carrier, general aviation, etc.) and phase (ground taxiing, takeoff, approach, enroute, transoceanic, landing, etc.). Ambient conditions are those involving temperature, humidity, lightning, electromagnetic effects, radiation, precipitation, vibration, etc.

SHELL Model of a system



S= Software (procedures, symbology, etc.)
H= Hardware (machine)
E= Environment (operational and ambient)
L= Liveware (human element)

Figure 3-6: The SHELL Model

In the SHELL model, the match or mismatch of the blocks (interface) is just as important as the characteristics described by the blocks themselves. These blocks may be re-arranged as required to describe the system. A connection between blocks indicates an interface between the two elements.

Each element of the system should be described both functionally and physically if possible. A function is defined as

An action or purpose for which a system, subsystem, or element is designed to perform.

Functional description: A functional description should describe what the system is intended to do, and should include subsystem functions as they relate to and support the system function. Review the FAA System Engineering Manual (SEM) for details on functional analysis.

Physical characteristics: A physical description provides the audience with information on the real composition and organization of the tangible system elements. As before, the level of detail varies with the size and complexity of the system, with the end objective being adequate audience understanding of the safety risk.

Both models describe interfaces. These interfaces come in many forms. The table below is a list of interface types that the system engineer may encounter.

Interface Type	Examples
Mechanical	Transmission of torque via a driveshaft. Rocket motor in an ejection seat.
Control	A control signal sent from a flight control computer to an actuator. A human operator selecting a flight management system mode.
Data	A position transducer reporting an actuator movement to a computer. A cockpit visual display to a pilot.
Physical	An avionics rack retaining several electronic boxes and modules. A computer sitting on a desk. A brace for an air cooling vent. A flapping hinge on a rotor.
Electrical	A DC power bus supplying energy to an anti-collision light. A fan plugged into an AC outlet for current. An electrical circuit closing a solenoid.
Aerodynamic	A stall indicator on a wing. A fairing designed to prevent vortices from impacting a control surface on an aircraft.
Hydraulic	Pressurized fluid supplying power to an flight control actuator. A fuel system pulling fuel from a tank to the engine.
Pneumatic	An adiabatic expansion cooling unit supplying cold air to an avionics bay. An air compressor supplying pressurized air to an engine air turbine starter.
Electromagnetic	RF signals from a VOR . A radar transmission.

ⁱ MIL-STD-882. (1984). Military standard system safety program requirements. Department of Defense.